**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Group Art Unit: Unknown
Examiner: Unknown

In re Patent Application of:

| | | |
|---|---|---|
| Applicant(s) | : SCHEIDT et al. | ) |
| Serial No. | : Unknown | ) |
| Filed | : Herewith | ) **PRELIMINARY** |
| | | ) **AMENDMENT** |
| For | : CRYPTOGRAPHIC KEY SPLIT COMBINER | ) |
| Attorney Ref. | : STS 119D1 | ) |

Commissioner for Patents
Washington, D.C. 20231

Sir:

Please amend the above-referenced application as follows:

**IN THE SPECIFICATION:**

Please amend the specification as follows:

Page 1, prior to "**Field of the Invention**", please insert the following heading and paragraph:

--**Cross-Reference to Related Applications**

This is a divisional of U.S. patent application Ser. No. 09/023,672, entitled "Cryptographic Key Split Combiner", filed February 13, 1998, the disclosure of which is

incorporated herein by reference, and the benefit of the filing date of which is claimed under 35 U.S.C. §120.--

**IN THE CLAIMS:**

Please cancel claims 1, 2, 35, 36, and 66 without prejudice or disclaimer to the subject matter recited therein, and amend the claims to read as follows:

3. (Amended) A cryptographic key split combiner, comprising:

a plurality of key split generators for generating cryptographic key splits; and

a key split randomizer for randomizing the cryptographic key splits to produce a cryptographic key;

wherein each of said key split generators includes means for generating key splits from seed data;

wherein said plurality of key split generators includes a random split generator for generating a random key split based on reference data; and

wherein said random split generator includes means for generating a random sequence based on the reference data.

4. (Amended) The cryptographic key split combiner of claim 3, wherein said random split generator includes means for generating a pseudorandom sequence based on the reference data.

5. (Amended) The cryptographic key split combiner of claim 3, wherein said random split generator includes means for generating a key split based on the reference data and on chronological data.

6. (Amended) The cryptographic key split combiner of claim 3, wherein said random split generator includes means for generating a key split based on the reference data and on static data.

9. (Amended) The cryptographic key split combiner of claim 3, wherein said plurality of key split generators includes a token split generator for generating a token key split based on label data.

18. (Amended) The cryptographic key split combiner of claim 3, wherein said plurality of key split generators includes a console split generator for generating a console key split based on maintenance data.

25. (Amended) The cryptographic key split combiner of claim 3, wherein said plurality of key split generators includes a biometric split generator for generating a biometric key split based on biometric data.

32. (Amended) The cryptographic key split combiner of claim 3, wherein the cryptographic key is a stream of symbols.

33. (Amended) The cryptographic key split combiner of claim 3, wherein the cryptographic key is at least one symbol block.

34. (Amended) The cryptographic key split combiner of claim 3, wherein the cryptographic key is a key matrix.

37. (Amended) A process for forming cryptographic keys, comprising:

generating a plurality of cryptographic key splits from seed data; and

randomizing the cryptographic key splits to produce a cryptographic key;

wherein generating a plurality of cryptographic key splits includes generating a random key split based on reference data; and

wherein generating a random key split includes generating a random sequence based on the reference data.

38. (Amended) The process of claim 37, wherein generating a random key split includes generating a pseudorandom sequence based on the reference data.

39. (Amended) The process of claim 37, wherein generating a random key split includes generating a key split based on the reference data and on chronological data.

40. (Amended) The process of claim 37, wherein generating a random key split includes generating a key split based on the reference data and on static data.

43. (Amended) The process of claim 37, wherein generating a plurality of cryptographic key splits includes generating a token key split based on label data.

52. (Amended) The process of claim 37, wherein generating a plurality of cryptographic key splits includes generating a console key split based on maintenance data.

59. (Amended) The process of claim 37, wherein generating a plurality of cryptographic key splits includes generating a biometric key split based on biometric data.

67. (Amended) A cryptographic key, including a stream of symbols, formed by the process of:

generating a plurality of cryptographic key splits from seed data; and

randomizing the cryptographic key splits to produce a cryptographic key.

68. (Amended) The cryptographic key of claim 67, including at least one symbol block.

69. (Amended) The cryptographic key of claim 67, including a key matrix.

## REMARKS

Claims 1-69 were filed in the application. Claims 1, 2, 35, 36, and 66 are canceled. Claims 3-6, 9, 18, 25, 32-34, 37-40, 43, 52, 59, and 67-69 are amended. Claims 3, 37, and 67 are the independent claims. Please enter the Preliminary Amendment prior to calculating the filing fee.

The parent application is under appeal. In that application, claims 1, 2, 35, 36, and 66 remain rejected and under appeal, and claims 3-34, 37-65, and 67-69 are objected to. Therefore, claims 3, 37, and 67 are presented in independent form, and dependent claims are amended accordingly as necessary, for proper dependence. Please note that, because claims 3, 37, and 67 originally included, through dependence, all the limitations added explicitly by this Amendment, the claims have not been substantively amended.

Consideration of the amended application is respectfully requested.

Respectfully submitted,

June 6, 2001
Date

Thomas M. Champagne
Registration No. 36,478
RABIN & CHAMPAGNE, P.C.
1101 14th Street, N.W., Suite 500
Washington, D.C. 20005
(202) 659-1915
(202) 659-1898 fax

TMC:lep

## Version With Markings To Show Changes Made

1. (Canceled)

2. (Canceled)

3. (Amended) [The] A cryptographic key split combiner, comprising: [of claim 2,]

a plurality of key split generators for generating cryptographic key splits; and

a key split randomizer for randomizing the cryptographic key splits to produce a cryptographic key;

wherein each of said key split generators includes means for generating key splits from seed data;

wherein said plurality of key split generators includes a random split generator for generating a random key split based on reference data; and

wherein said random split generator includes means for generating a random sequence based on the reference data.

4. (Amended) The cryptographic key split combiner of claim [2] 3, wherein said random split generator includes means for generating a pseudorandom sequence based on the reference data.

5. (Amended) The cryptographic key split combiner of claim [2] 3, wherein said random split generator includes means for generating a key split based on the reference data and on chronological data.

6. (Amended) The cryptographic key split combiner of claim [2] 3, wherein said random split generator includes means for generating a key split based on the reference data and on static data.

9. (Amended) The cryptographic key split combiner of claim [1] 3, wherein said plurality of key split generators includes a token split generator for generating a token key split based on label data.

18. (Amended) The cryptographic key split combiner of claim [1] 3, wherein said plurality of key split generators includes a console split generator for generating a console key split based on maintenance data.

25. (Amended) The cryptographic key split combiner of claim [1] 3, wherein said plurality of key split generators includes a biometric split generator for generating a biometric key split based on biometric data.

32. (Amended) The cryptographic key split combiner of claim [1] 3, wherein the cryptographic key is a stream of symbols.

33. (Amended) The cryptographic key split combiner of claim [1] 3, wherein the cryptographic key is at least one symbol block.

34. (Amended) The cryptographic key split combiner of claim [1] 3, wherein the cryptographic key is a key matrix.

35. (Canceled)

36. (Canceled)

37. (Amended) [The] A process [of claim 36,] for forming cryptographic keys, comprising:

generating a plurality of cryptographic key splits from seed data; and

randomizing the cryptographic key splits to produce a cryptographic key;

wherein generating a plurality of cryptographic key splits includes generating a random key split based on reference data; and

wherein generating a random key split includes generating a random sequence based on the reference data.

38. (Amended) The process of claim [36] 37, wherein generating a random key split includes generating a pseudorandom sequence based on the reference data.

39. (Amended) The process of claim [36] 37, wherein generating a random key split includes generating a key split based on the reference data and on chronological data.

40. (Amended) The process of claim [36] 37, wherein generating a random key split includes generating a key split based on the reference data and on static data.

43. (Amended) The process of claim [35] 37, wherein generating a plurality of cryptographic key splits includes generating a token key split based on label data.

52. (Amended) The process of claim [35] 37, wherein generating a plurality of cryptographic key splits includes generating a console key split based on maintenance data.

59. (Amended) The process of claim [35] 37, wherein generating a plurality of cryptographic key splits includes generating a biometric key split based on biometric data.

66. (Canceled)

67. (Amended) [The] A cryptographic key [of claim 66], including a stream of symbols, formed by the process of:

generating a plurality of cryptographic key splits from seed data; and

randomizing the cryptographic key splits to produce a cryptographic key.

68. (Amended) The cryptographic key of claim [66] 67, including at least one symbol block.

69. (Amended) The cryptographic key of claim [66] 67, including a key matrix.